Using Instant Messaging and Chat Rooms Safely

Cyber Security Tip ST04-011

Although they offer a convenient way to communicate with other people, there are dangers associated with tools that allow real-time communication.

What are the differences between some of the tools used for real-time communication?

- Instant messaging (IM) - Commonly used for recreation, instant messaging is also becoming more widely used within corporations for communications between employees. IM, regardless of the specific software you choose, provides an interface for individuals to communicate one-on-one.
- Chat rooms - Whether public or private, chat rooms are forums for particular groups of people to interact. Many chat rooms are based upon a shared characteristic; for example, there are chat rooms for people of particular age groups or interests. Although most IM clients support "chats" among multiple users, IM is traditionally one-to-one while chats are traditionally many-to-many.
- Bots - A "chat robot," or "bot," is software that can interact with users through chat mechanisms, whether in IM or chat rooms. In some cases, users may be able to obtain current weather reports, stock status, or movie listings. In these instances, users are often aware that they are not interacting with an actual human. However, some users may be fooled by more sophisticated bots into thinking the responses they are receiving are from another person.

There are many software packages that incorporate one or more of these capabilities. A number of different technologies might be supported, including IM, Internet Relay Chat (IRC), or Jabber.

What are the dangers?

- Identities can be elusive or ambiguous - Not only is it sometimes difficult to identify whether the "person" you are talking to is human, but human nature and behavior isn't predictable. People may lie about their identity, accounts may be compromised, users may forget to log out, or an account may be shared by multiple people. All of these things make it difficult to know who you're really talking to during a conversation.
- Users are especially susceptible to certain types of attack - Trying to convince someone to run a program or click on a link is a common attack method, but it can be especially effective through IM and chat rooms. In a setting where a user feels comfortable with the "person" he or she is talking to, a malicious piece of software or an attacker has a better chance of convincing someone to fall into the trap (see Avoiding Social Engineering and Phishing Attacks for more information).
- You don't know who else might be seeing the conversation – Online interactions are easily saved, and if you're using a free commercial service the exchanges may be archived on a server. You have no control over what happens to those logs.

You also don't know if there's someone looking over the shoulder of the person you're talking to, or if an attacker might be "sniffing" your conversation.

- The software you're using may contain vulnerabilities - Like any other software, chat software may have vulnerabilities that attackers can exploit.
- Default security settings may be inappropriate - The default security settings in chat software tend to be relatively permissive to make it more open and "usable," and this can make you more susceptible to attacks.

How can you use these tools safely?

- Evaluate your security settings - Check the default settings in your software and adjust them if they are too permissive. Make sure to disable automatic downloads. Some chat software offers the ability to limit interactions to only certain users, and you may want to take advantage of these restrictions.
- Be conscious of what information you reveal - Be wary of revealing personal information unless you know who you are really talking to. You should also be careful about discussing anything you or your employer might consider sensitive business information over public IM or chat services (even if you are talking to someone you know in a one-to-one conversation).
- Try to verify the identity of the person you are talking to, if it matters - In some forums and situations, the identity of the "person" you are talking to may not matter. However, if you need to have a degree of trust in that person, either because you are sharing certain types of information or being asked to take some action like following a link or running a program, make sure the "person" you are talking to is actually that person.
- Don't believe everything you read - The information or advice you receive in a chat room or by IM may be false or, worse, malicious. Try to verify the information or instructions from outside sources before taking any action.
- Keep software up to date - This includes the chat software, your browser, your operating system, your mail client, and, especially, your anti-virus software (see Understanding Patches and Understanding Anti-Virus Software for more information).

Authors: Mindi McDowell, Allen Householder

Produced 2004 by US-CERT, a government organization.

Note: This tip was previously published and is being re-distributed to increase awareness.

This document can also be found at http://www.us-cert.gov/cas/tips/ST04-011.html